



MISSILE DEFENSE AGENCY

ANTI-TAMPER POLICY

DIRECTIVE 5200.05

July 18, 2006

Office of Primary Responsibility: Deputy for Engineering (MDA/DE)

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1. REISSUANCE AND PURPOSE.....	3
2. APPLICABILITY AND SCOPE.....	4
3. DEFINITIONS.....	4
4. POLICY.....	5
5. RESPONSIBILITIES.....	8
6. EFFECTIVE DATE.....	10

ENCLOSURES

- EN1. Enclosure 1, MDA ANTI-TAMPER SPIRAL PROCESS
- EN2. Enclosure 2, MDA ANTI-TAMPER REVIEW/APPROVAL PROCESS
- EN3. Enclosure 3, ANTI-TAMPER RELATED ANALYSIS FOR SDR
- EN4. Enclosure 4, ANTI-TAMPER RELATED ANALYSIS FOR PDR
- EN5. Enclosure 5, ANTI-TAMPER RELATED ANALYSIS FOR CDR
- EN6. Enclosure 6, ANTI-TAMPER RELATED ANALYSIS FOR COMPLETION
INTEGRATED DEVELOPMENT TESTING



**DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY**
7100 DEFENSE PENTAGON
WASHINGTON, DC 20301-7100

DE

MDA DIRECTIVE 5200.05

SUBJECT: Anti-Tamper Policy

References: (a) Missile Defense Agency Directive 5200.03, "Anti-Tamper Program, August 23, 2004 (hereby cancelled).
(b) Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) Memorandum "Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs," 1 May 2000.
(c) Assistant Secretary of the Air Force for Acquisition "Safe Array Compartment Security Classification Guide (U)," 11 Jul 05.
(d) Office of the Secretary of Defense, "Interim Defense Acquisition Guidebook," 30 Oct 30 2002.
(e) DoDD 5200.39, "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection," 10 September 1997
(f) DoD 5200.1-M, "Acquisition Systems Protection Program," March, 1994

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policy and responsibilities. This Directive also institutes discipline in the development and implementation of Anti-Tamper (AT) technologies to protect Critical Program Information (CPI) from unintentional transfer for Ballistic Missile Defense System (BMDS) programs.

1.2. Establishes the Missile Defense Agency (MDA) AT procedures (including AT deliverables, milestones, and approvals), organizational responsibilities, and interfaces required to effectively execute this Directive.

1.3. Establishes the MDA Anti-Tamper Working Group to oversee and coordinate AT activities across the Missile Defense Agency (MDA).

1.4. Establishes accountability in implementing AT procedures and applying AT technologies to protect critical technologies.

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to all MDA Ballistic Missile Defense acquisition programs and associated technology programs (hereafter referred to collectively as "the MDA Programs").

2.2. In case of conflict between this document and Law or Government/Service regulations, the stricter requirement shall govern unless otherwise waived.

3. DEFINITIONS

3.1. Anti-Tamper (AT). MDA program engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. Weapon Systems. The purpose is to add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or component.

3.2. Critical Program Information (CPI). Classified or unclassified program information, technologies, or systems that, if compromised, would: (1) degrade combat effectiveness, (2) shorten the expected combat effective life of the system, or (3) significantly alter program direction.

3.3. Program Protection Plan (PPP). The PPP is the program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to CPI to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access. Additional guidance on Program Protection Planning, Technology Protection, and Anti-Tamper may be found in the references (e) and (f), as well as in the Defense Acquisition Guidebook (DAG) website at <http://akss.dau.mil/dag>.

3.4. Unintentional Transfer. Transfer of technology as a result of battlefield loss or transfer of technology occurring outside of what is specified and planned in memoranda of understanding and/or agreements (signed between the United States and other nations) which govern co-development, co-production, or foreign military sales.

3.5. Completion of Integrated Development Testing. In concert with Verification and Validation, Completion of Integrated Development Testing ensures that AT implementation does not have any unintended consequences for normal operation of the weapon system. Although some early Verification and Validation activities can be accomplished prior to full weapon system integration, integrated development testing is required to reduce risk.

3.6. Verification. The analysis, inspection, demonstration, and test of AT measures that were stipulated in the AT Plan, as well as the determination that the AT within the system operates according to the AT developer's specifications. (i.e., Are we building the product right? Does the AT system work as intended? Did we implement the AT correctly in the system?)

3.7. Validation. The process of determining that the AT implementation will fulfill its intended function. (i.e., Are we building the right product? Does the Anti-Tamper Plan satisfy the AT requirements?)

4. POLICY

The MDA Programs shall adhere to the AT procedures of this Directive summarized as follows.

4.1. Timeline.

4.1.1. Entrance Criteria. For each Program milestone described in enclosure 1, the entrance criteria is the submission of the AT product required (as described below) 60-days prior to the milestone.

4.1.2. Exit Criteria. No milestone can be considered successfully completed without satisfying the exit criteria of having the AT product approved in accordance with the procedures illustrated in enclosure 2.

4.2. Anti-Tamper Plan.

4.2.1. AT Design Concept. MDA Programs must document CPI and perform appropriate analysis to determine if the CPI is at risk of unintentional transfer and, therefore, must be provided AT protection. This analysis must be performed as early in the program development spiral as practical and must be performed in a manner sufficient to meet the AT approval milestone schedule requirements (for example, prior to a System (Concept) Design Review (SDR) or Preliminary Design Review (PDR), as illustrated in enclosures 3 and 4). Analysis to determine CPI risk should include, but is not limited to: the identification of impacts if exploited, needed protection timelines, threat scenarios, vulnerabilities, AT maintenance and logistics requirements, attack tree analysis, available AT technologies, potential AT solutions, and AT designs and funding requirements.

4.2.2. Responsibility. Program managers and officials in program oversight roles must adhere to the processes and procedures defined in this Directive to ensure that the required AT deliverables and technologies provide an effective, risk-based, cost-effective

AT program. It is essential that AT design efforts are initiated as early as possible in the acquisition life cycle; however, regardless of when an AT program is established, every effort must be made to incorporate AT measures where appropriate, considering the overall risk of the loss of critical information or technology.

4.2.3. Initial AT Plan. The initial AT plan shall document the program's CPI analysis as outlined in Section 4.2.1., proposed AT measures, and must include other documentation as required by Department of Defense (DoD) policy.

4.2.4. Final AT Plan. The AT Plan, which is a classified annex to the PPP, shall document the potential AT reverse engineering threats, vulnerabilities, and mitigation techniques, and analysis to determine CPI risk. The plan must include a final AT design with attendant programmatic estimates (cost, schedule, performance, and risk). Prior to the Critical Design Review (CDR), the Program must have completed for approval a final AT plan and AT verification plan as outlined in Section 4.5. and attached enclosures.

4.2.5. AT Plan Template. The AT Plan Template is available from the MDA AT Executive.

4.3. Verification. All AT products are submitted for approval to the MDA AT Executive for coordination with the DoD AT Executive Agent. MDA approval and DoD coordination is facilitated by an Anti-Tamper Working Group (as described below).

4.3.1. Verification Plan Content. The verification plan must include descriptions of testing objectives, methodology, and expected outcomes that will verify the effectiveness of the AT design. AT system verification plans, including, for example, test objectives, test descriptions, test methodology, and expected outcomes, must also be developed in accordance with reference (b).

4.3.2. Reporting. Prior to completion of integrated development testing (enclosure 6), all AT verification testing must be successfully completed and an AT verification report submitted to the MDA Executive for approval.

4.3.3. Documentation. AT verification plans shall reside in the Developmental Master Test Plans. AT shall also be cross-referenced in the System Engineering Plan where appropriate and consistent with other systems engineering planning and in other relevant acquisition documents to include the Acquisition Strategy Report and the Acquisition Program Baseline.

4.3.4. Verification Plan Template. The Verification Plan Template is available from the MDA AT Executive.

4.4. Anti-Tamper Working Group. MDA will establish an Anti-Tamper Working Group to be led by the MDA AT Executive.

4.4.1. Duties. The Anti-Tamper Working Group shall coordinate AT activities across MDA and with the DoD Executive AT Agent and provide programs advice and guidance. The Anti-Tamper Working Group will review all MDA program AT deliverables prior to submission for MDA approval and concurrence by the DoD AT Executive Agent (or designated representative). The Anti-Tamper Working Group will monitor the MDA AT effort and develop additional or modify existing guidance, as necessary.

4.4.2. Members. The Anti-Tamper Working Group, led by the MDA AT Executive, will include representatives from the Executive Director (MDA/DX); System Engineering & Integration Directorate (MDA/DEE); Quality, Safety & Mission Assurance Directorate (MDA/QS); Security/Intelligence Operations Directorate (MDA/DOS); Producibility and Mantech Directorate (MDA/DEP); Deputy for International Affairs (MDA/DI); Deputy for Agency Operations (MDA/DO); Deputy for Test (MDA/DT); BMDS Elements; DoD AT Executive Agent; national labs; research centers; advisory panels; and others as appropriate.

4.5. Approval. The MDA Anti-Tamper development and approval process is summarized in enclosure 1. AT development milestones (which satisfy the recommended DoD AT process) are intended to correspond to Program maturity milestones including SDR, PDR, CDR, and Completion of Integrated Development Testing. This AT development process is completed for each system development spiral.

4.5.1. AT Executive Agent. The Deputy for Engineering (MDA/DE) shall serve as the Missile Defense Agency Anti-Tamper Executive. Milestone Decision Authority for AT products and approval of all AT deliverables is delegated by the Director to the AT Executive. The signature authority for AT deliverables remains with the program manager; however, the Anti-Tamper Working Group will coordinate the MDA review and DoD AT Executive Agent concurrence of deliverables prior to submission to the decision authority, the MDA AT Executive. The MDA AT Executive will approve or disapprove AT implementation. In accordance with paragraph 4.6. below, if an AT plan or its approved implementation is revised or altered by a program at any time, then the associated AT deliverables shall be resubmitted to the Anti-Tamper Working Group for another cycle of the review and approval process. In addition, the MDA Programs shall brief current and planned AT activities at all program reviews, including System Element Reviews, and decision points as identified by the Anti-Tamper Working Group during their review of program plans and schedules.

4.6. Security Coordination. As soon as AT requirements are identified, and throughout the AT development process, MDA Programs shall coordinate with

MDA/DOS to evaluate AT special access security requirements and establish the required security controls.

4.7. Transition. As the MDA Programs evolve and prepare for transition to the Services, the Anti-Tamper Working Group, in conjunction with the AT Service Leads, will provide guidance necessary for programs to follow Service Anti-Tamper policies and procedures.

5. RESPONSIBILITIES

5.1. The Deputy for Engineering (MDA/DE) will:

5.1.1. Serve as the MDA AT Executive.

5.1.2. Chair the Anti-Tamper Working Group.

5.1.3. Be responsible to the Director, MDA (MDA/D) for establishing and implementing AT policy.

5.1.4. Act as the decision authority for AT options and deliverables.

5.1.5. Act as liaison to the DoD AT Executive Agent.

5.1.6. Advocate the funding of AT across MDA Programs.

5.1.7. Shall ensure affordability and appropriateness of proposed AT solutions.

5.2. The Producibility and Mantech Directorate (MDA/DEP) will:

5.2.1. Act as the Anti-Tamper Working Group Executive Secretary and will be responsible to MDA/DE for coordinating Element reviews, serving as the primary MDA interface with the DoD AT Executive Agent, defining resources required to sustain AT policy implementation, supporting the Services in understanding and transitioning Element AT activities, and serving as the MDA AT information conduit.

5.2.2. Provide and maintain a central repository for AT data to be used as a resource for MDA program managers, gathering information on AT points of contact, technologies, and techniques, and leading the development of generic AT technologies applicable to MDA AT implementation.

5.3. The System Engineering & Integration Directorate (MDA/DEE) will support the AT Executive in the development of AT requirements and specifications for implementing AT policy.

5.4. The Security/Intelligence Operations Directorate (MDA/DOS) will be responsible to the Director, MDA, for security, intelligence, counterintelligence, and special programs support to MDA AT efforts. The MDA Special Access Program Central Office (SAPCO) shall be responsible for ensuring special access protection of AT applications horizontally across the MDA Programs and of all associated documentation. The SAPCO shall support MDA/DE in serving as the focal point for access to the larger DoD AT special access community. MDA/DOS will assess security planning and implementation across all MDA Programs and will coordinate with other DoD agencies as required to ensure compliance with DoD policies for horizontal protection of AT information and documentation. MDA/DOS will ensure MDA compliance with DoD policies regarding security of AT technologies and implementing plans and will ensure that AT security is applied consistently across all MDA Programs.

5.5. The Deputy for International Affairs (MDA/DI) will provide guidance regarding international participation in MDA Programs and review of AT deliverables.

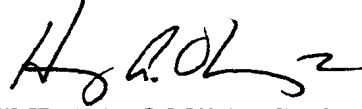
5.6. The Deputy for Agency Operations (MDA/DO) will be responsible to MDA/DE for conducting AT affordability assessments to include developing and/or reviewing cost estimates.

5.7. Anti-Tamper Working Group Members will be responsible for coordinating AT activities across MDA and providing programs advice and guidance. Members shall review all MDA Program AT deliverables prior to submission for concurrence to the DoD AT Executive Agent (or designated representative). In this capacity, they will provide the agency oversight necessary for AT to be implemented successfully from program initiation, through design, to fielding and/or transfer to the Services. As outlined herein, the Anti-Tamper Working Group Charter will serve as the authority for Anti-Tamper Working Group roles and responsibilities.

5.8. Program Directors will be responsible for adhering to the applicable requirements of this Directive and guidelines issued by the DoD AT Executive Agent to provide the BMDS necessary and appropriate AT protection.

6. EFFECTIVE DATE

This Directive is effective immediately.



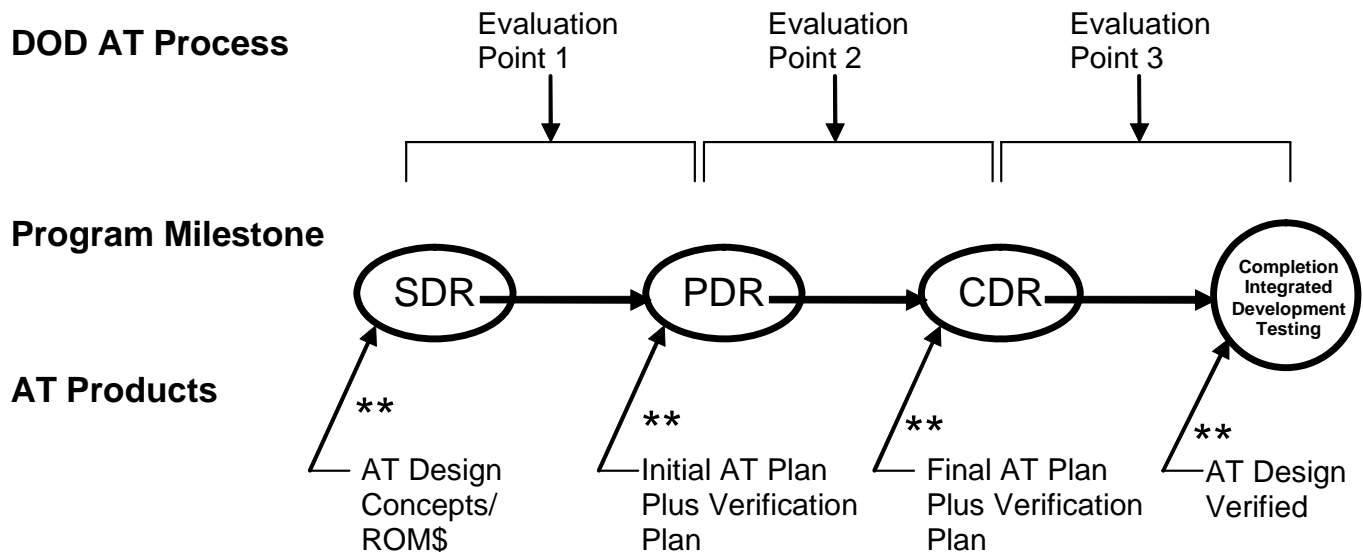
HENRY A. OBERING III
Lieutenant General, USAF
Director

Enclosures – 6

- E1. MDA Anti-Tamper Spiral Process
- E2. MDA Anti-Tamper Review/Approval Process
- E3. Anti-Tamper Related Analysis For SDR
- E4. Anti-Tamper Related Analysis For PDR
- E5. Anti-Tamper Related Analysis For CDR
- E6. Anti-Tamper Related Analysis For Completion Integrated Development Testing

E1. ENCLOSURE 1

MDA ANTI-TAMPER SPIRAL PROCESS*



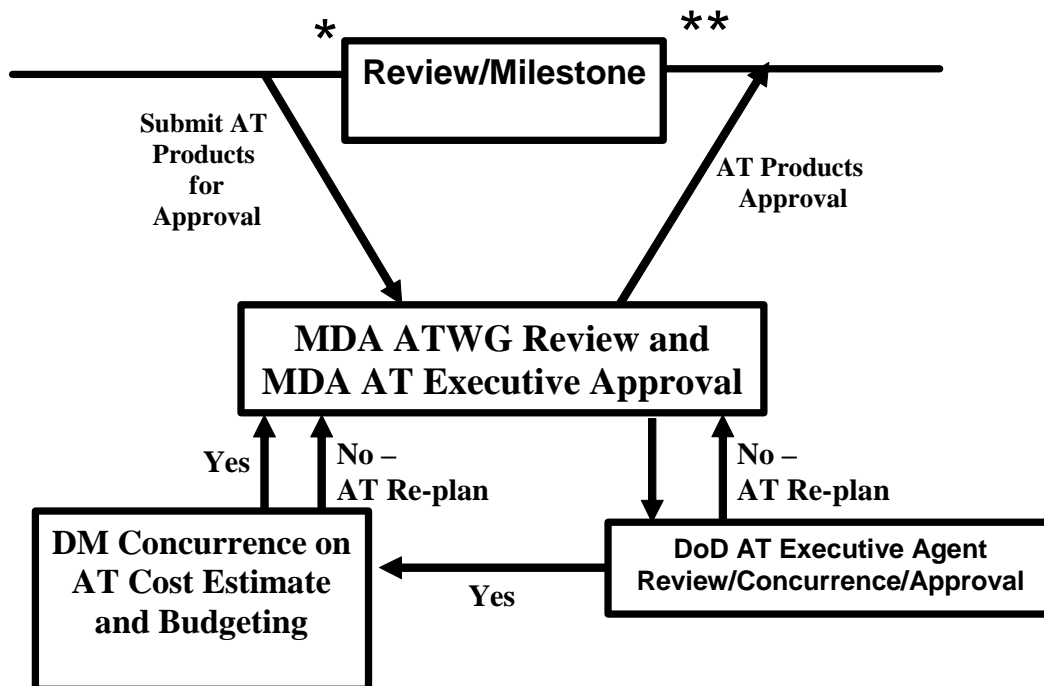
* Process applies to each capability spiral.

** Entrance Criteria: AT product due 60 days before Review/Milestone for review and approval.

Exit Criteria: AT Product approved (See Enclosure 2 for Approval Process)

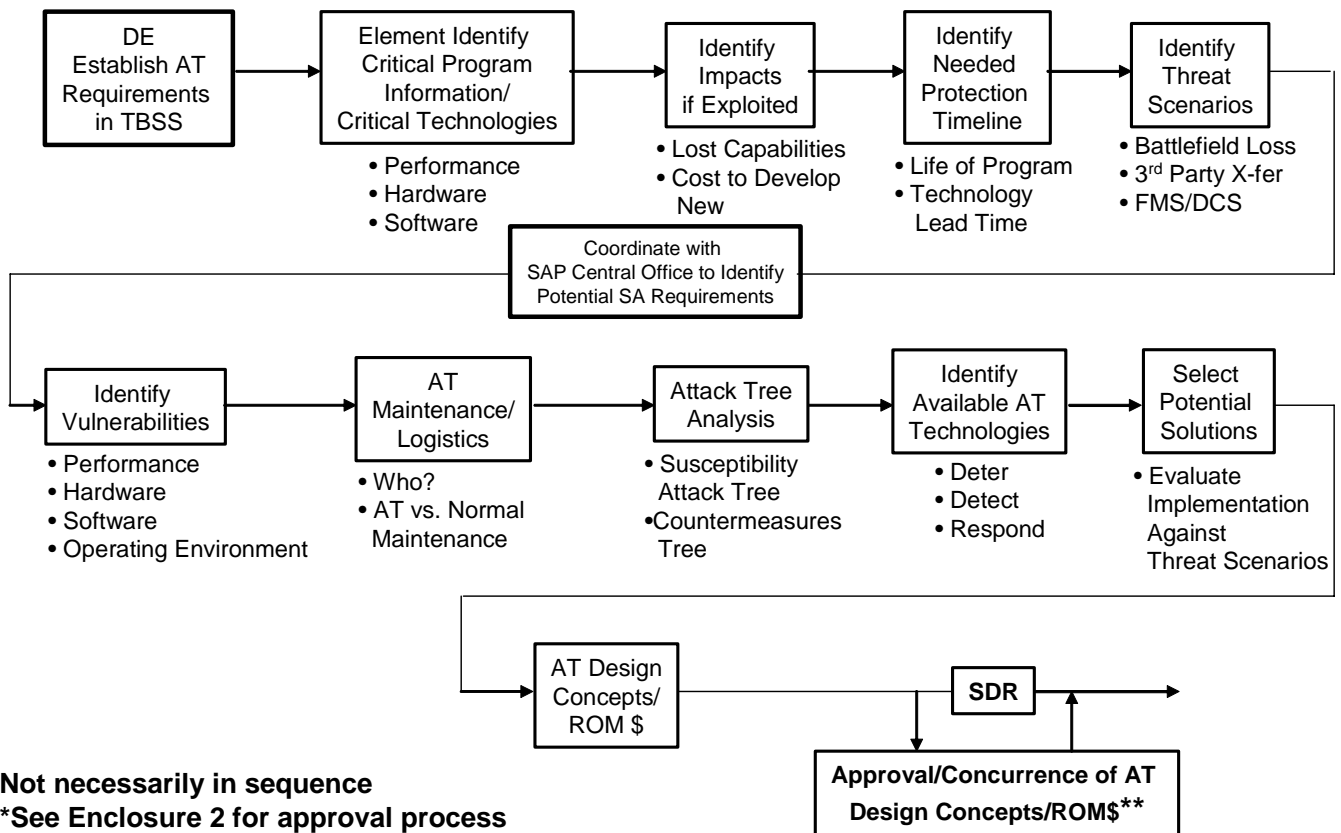
E2. ENCLOSURE 2

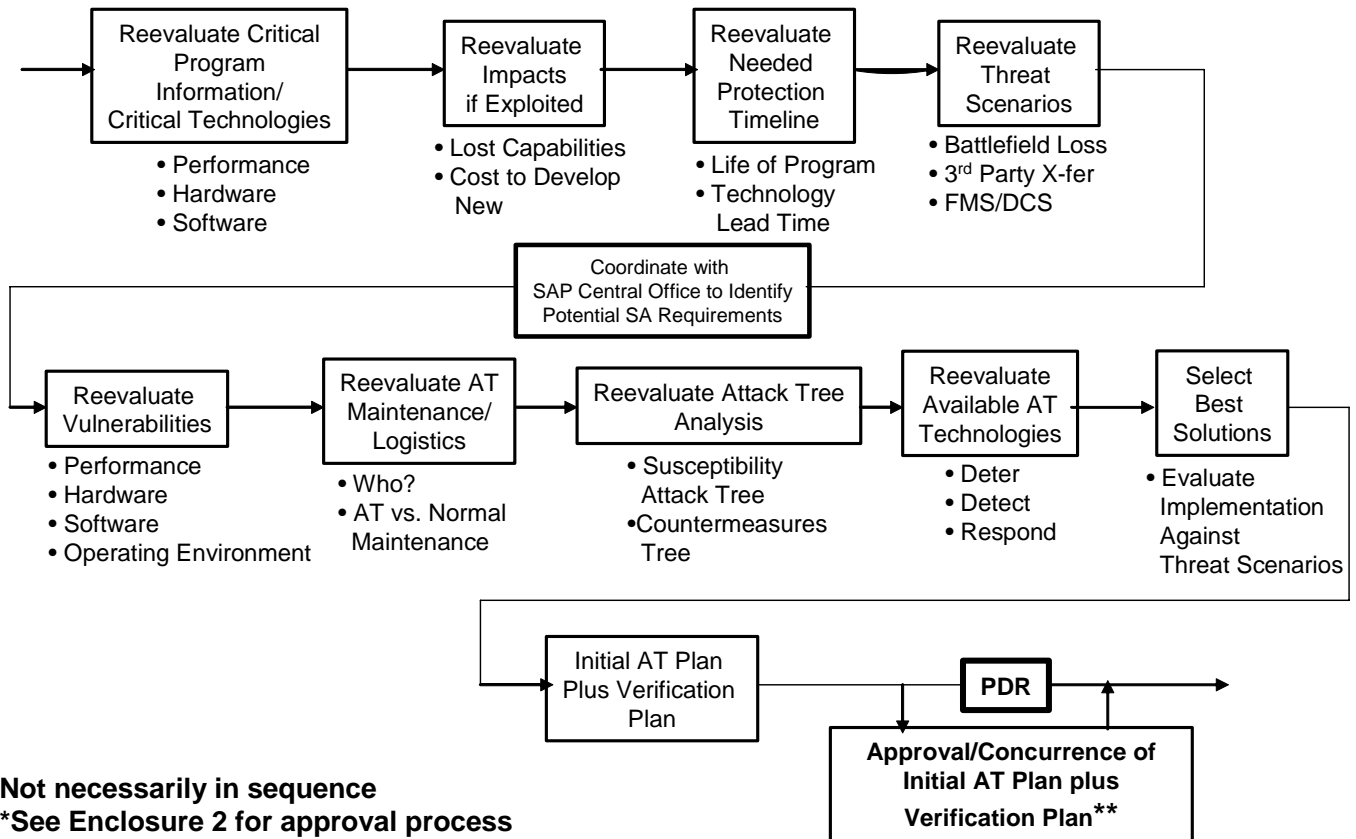
MDA ANTI-TAMPER REVIEW/APPROVAL PROCESS



* Review/Milestone entrance criteria includes submission of plan for review and approval

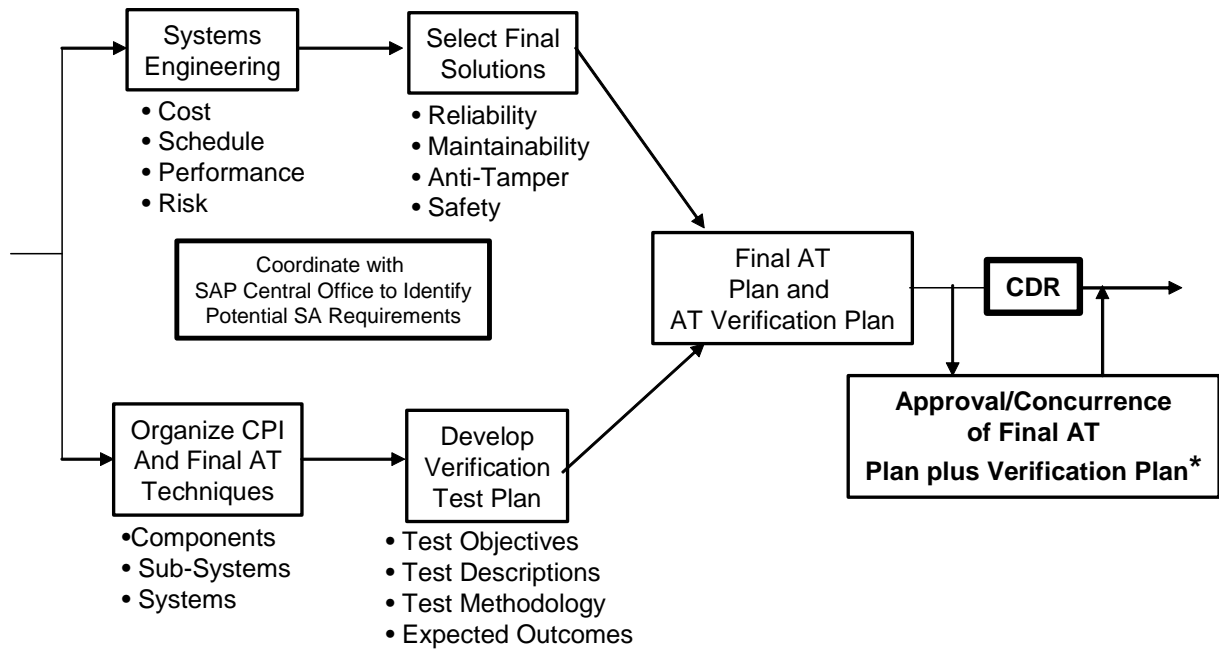
** Review/Milestone exit criteria includes approval of plan

E3. ENCLOSURE 3ANTI-TAMPER RELATED ANALYSIS FOR SDR*

E4. ENCLOSURE 4ANTI-TAMPER RELATED ANALYSIS FOR PDR*

E5. ENCLOSURE 5

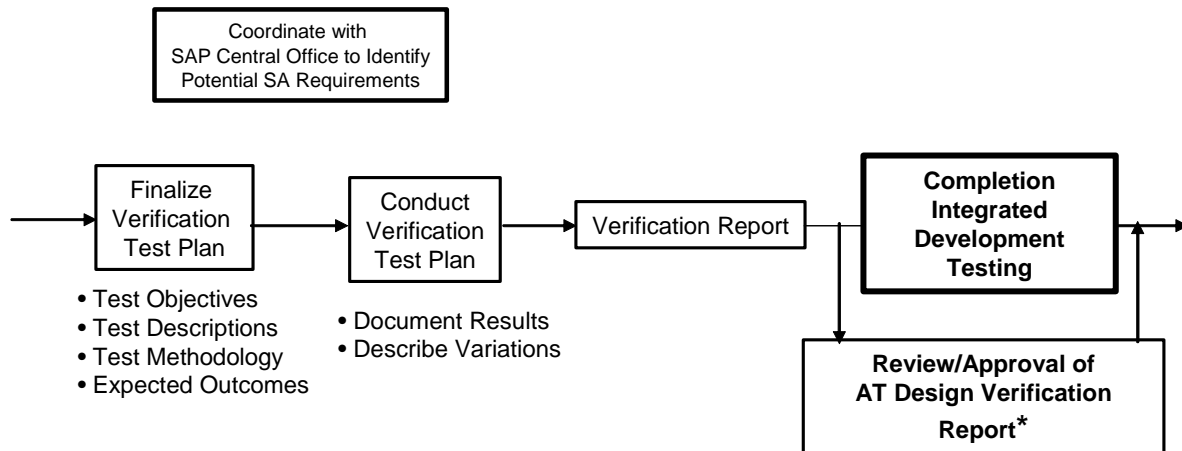
ANTI-TAMPER RELATED ANALYSIS FOR CDR



* See Enclosure 2 for approval process

E6. ENCLOSURE 6

ANTI-TAMPER RELATED ANALYSIS FOR COMPLETION INTEGRATED
DEVELOPMENT TESTING



* See Enclosure 2 for approval process